CLAIMS

What is claimed is:

1. A method of securely establishing a call between a first node of a voice over Internet Protocol call connection and a second node thereof, the method comprising the computer-implemented steps of:
receiving non-encrypted authentication request information from the first node;
receiving, from an authentication server that is communicatively coupled to the second node, an authentication message indicating whether the first node is authenticated based on the non-encrypted authentication request information;
establishing a call between the second node and the first node only when the authentication message indicates that the first node is authenticated at the authentication server.

2. A method as recited in Claim 1, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an access token comprising a general identifier value, a time stamp value, a challenge value, and a random value.

3. A method as recited in Claim 1, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an H.235 ClearToken comprising a general identifier value, a time stamp value, a challenge value, and a random value.

4. A method as recited in Claim 1, wherein the step of receiving non-encrypted authentication request information further comprises the steps of:
determining whether the authentication request information was created within a reasonable time with respect to the then-current time;

issuing a request for authentication to the authentication server only when the authentication request information was created within a reasonable time with respect to the then-current time.

5. The method as recited in Claim 1, further comprising the steps of:
receiving a password that is associated with the first node;
generating an authentication response based on the password and challenge information contained in the authentication request information;
determining whether the authentication response matches the authentication request information;
issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information.

6. The method as recited in Claim 1, further comprising the steps of:
receiving a password that is associated with the first node;
generating a Challenge Handshake Authentication Protocol (CHAP) response based on the password and implied CHAP challenge information contained in the authentication request information;
determining whether the authentication response matches the authentication request information based on CHAP;
issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information based on CHAP.

7. A method of securely establishing a call in a voice over Internet Protocol call connection system that includes a first gateway at a call origination point, a first gatekeeper, a second gatekeeper, a second gateway at a call termination point, and an authentication server that is communicatively coupled to the first gatekeeper and the second gatekeeper, the method comprising the computer-implemented steps of:
receiving non-encrypted authentication request information from the first gateway;

receiving from the authentication server an authentication message indicating whether the first gateway is authenticated based on the non-encrypted authentication request information;

establishing a call between the second gateway and the first gateway only when the authentication message indicates that the first gateway is authenticated at the authentication server.

8. A method as recited in Claim 7, further comprising the steps of:

receiving a call setup request message at the first gateway;

creating and storing the non-encrypted authentication request information based on the current time and information that uniquely identifies the first gateway;

requesting the second gateway to set up a call based on the authentication request information.

9. A method as recited in Claim 8, further comprising the steps of:

determining whether the authentication request information was created within a reasonable time with respect to the then-current time at the second gatekeeper;

requesting the authentication server to carry out authentication of the first gateway only when the authentication request information was created within a reasonable time with respect to the then-current time at the second gatekeeper.

10. A method as recited in Claim 7, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an access token comprising a general identifier value, a time stamp value, a challenge value, and a random value.

11. A method as recited in Claim 7, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an H.235 ClearToken comprising a general identifier value, a time stamp value, a challenge value, and a random value.

12. The method as recited in Claim 7, further comprising the steps of:

receiving a password that is associated with the first gateway;

generating an authentication response based on the password and challenge information contained in the authentication request information;

determining whether the authentication response matches the authentication request information;

issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information.

13. The method as recited in Claim 7, further comprising the steps of:

receiving a password that is associated with the first gateway;

generating an authentication response based on the password and challenge information contained in the authentication request information;

determining whether the authentication response matches the authentication request information;

issuing authentication approval information in the authentication message to the second gatekeeper only when the authentication response matches the authentication request information;

issuing authentication rejection information in the authentication message to the second gatekeeper when the authentication response does not match the authentication request information.

14. The method as recited in Claim 7, further comprising the steps of:

receiving a password that is associated with the first gateway;

generating a Challenge Handshake Authentication Protocol (CHAP) response based on the password and implied CHAP challenge information contained in the authentication request information;

determining whether the authentication response matches the authentication request information based on CHAP;

issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information based on CHAP.

15. The method as recited in Claim 12, wherein the step of establishing a call between the second gateway and the first gateway comprises the step of establishing a call between the second gateway and the first gateway only when authentication approval information is received in the authentication message.

16. A method of securely establishing a call in a voice over Internet Protocol call connection system that includes a first gateway at a call origination point, a first gatekeeper, a second gatekeeper, a second gateway at a call termination point, and an authentication server that is communicatively coupled to the first gatekeeper and the second gatekeeper, the method comprising the computer-implemented steps of:

receiving user identification information from the first gateway that comprises a user identifier and a personal identification number that are uniquely associated with a calling party who originates a call using the first gateway;

receiving from the authentication server a first authentication message indicating whether the user identification information is authenticated;

receiving non-encrypted authentication request information from the first gateway;

receiving from the authentication server a second authentication message indicating whether the first gateway is authenticated based on the non-encrypted authentication request information;

establishing a call between the second gateway and the first gateway for the calling party only when the first authentication message indicates that the user identification information is authenticated and the second authentication message indicates that the first gateway is authenticated at the authentication server.

17. A method as recited in Claim 16, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an access token comprising a general identifier value, a time stamp value, a challenge value, and a random value.

18. A method as recited in Claim 16, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an H.235 ClearToken comprising a general identifier value, a time stamp value, a challenge value, and a random value.

19. A method as recited in Claim 16, wherein the step of receiving non-encrypted authentication request information further comprises the steps of:
determining whether the authentication request information was created within a reasonable time with respect to the then-current time;
issuing a request for authentication to the authentication server only when the authentication request information was created within a reasonable time with respect to the then-current time.

20. The method as recited in Claim 16, further comprising the steps of:
receiving a password that is associated with the first gateway;
generating an authentication response based on the password and challenge information contained in the authentication request information;
determining whether the authentication response matches the authentication request information;
issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information.

21. The method as recited in Claim 16, further comprising the steps of:
receiving a password that is associated with the first gateway;

generating a Challenge Handshake Authentication Protocol (CHAP) response based on the password and implied CHAP challenge information contained in the authentication request information;

determining whether the authentication response matches the authentication request information based on CHAP;

issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information based on CHAP.

22. A method as recited in Claim 16, wherein the step of receiving non-encrypted user identification information further comprises the steps of:

determining whether the user identification information was created within a reasonable time with respect to the then-current time;

issuing a request for authentication to the authentication server only when the user identification information was created within a reasonable time with respect to the then-current time.

23. The method as recited in Claim 16, further comprising the steps of:

retrieving a personal identification value that is associated with the user account number in the user identification information;

determining whether the personal identification value matches the personal identification number that is in the user identification information;

issuing authentication approval information in the authentication message only when the personal identification value matches the personal identification number that is in the user identification information.

24. A computer-readable medium carrying one or more sequences of instructions for securely establishing a call between a first node of a voice over Internet Protocol call connection and a second node thereof, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving non-encrypted authentication request information from the first node;

receiving, from an authentication server that is communicatively coupled to the second node, an authentication message indicating whether the first node is authenticated based on the non-encrypted authentication request information;

establishing a call between the second node and the first node only when the authentication message indicates that the first node is authenticated at the authentication server.

25. A computer-readable medium as recited in Claim 24, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an access token comprising a general identifier value, a time stamp value, a challenge value, and a random value.

26. A computer-readable medium as recited in Claim 24, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an H.235 ClearToken comprising a general identifier value, a time stamp value, a challenge value, and a random value.

27. A computer-readable medium as recited in Claim 24, wherein the step of receiving non-encrypted authentication request information further comprises the steps of:

determining whether the authentication request information was created within a reasonable time with respect to the then-current time;

issuing a request for authentication to the authentication server only when the authentication request information was created within a reasonable time with respect to the then-current time.

28. The computer-readable medium as recited in Claim 24, further comprising the steps of:

receiving a password that is associated with the first node;

generating an authentication response based on the password and challenge information contained in the authentication request information;

determining whether the authentication response matches the authentication request information;

issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information.

29. The computer-readable medium as recited in Claim 24, further comprising the steps of:
receiving a password that is associated with the first node;
generating a Challenge Handshake Authentication Protocol (CHAP) response based on the password and implied CHAP challenge information contained in the authentication request information;
determining whether the authentication response matches the authentication request information based on CHAP;
issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information based on CHAP.

30. An apparatus for securely establishing a call between a first node of a voice over Internet Protocol call connection and a second node thereof, which instructions, comprising:
means for receiving non-encrypted authentication request information from the first node;
means for receiving, from an authentication server that is communicatively coupled to the second node, an authentication message indicating whether the first node is authenticated based on the non-encrypted authentication request information;
establishing a call between the second node and the first node only when the authentication message indicates that the first node is authenticated at the authentication server.

31. An apparatus for securely establishing a call between a first node of a voice over Internet Protocol call connection and a second node thereof, comprising:
a network interface that is coupled to the data network for receiving one or more packet flows therefrom;
a processor;
one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving non-encrypted authentication request information from the first node;

receiving, from an authentication server that is communicatively coupled to the second node, an authentication message indicating whether the first node is authenticated based on the non-encrypted authentication request information;

establishing a call between the second node and the first node only when the authentication message indicates that the first node is authenticated at the authentication server.